IN THE CLAIMS

Please amend the claims as follows. This claim set is to replace all prior versions.

Listing Of The Claims:

1. (currently amended) A method of resetting a password for a network service account, the method comprising:

accepting entry of a password at a first server from an electronic device wherein the electronic device is remote from the first server;

comparing the entered password with a known password;

after comparing the entered password with the known password, redirecting ~~the~~ a user of the electronic device from the first server to a second server providing a password reset tool if the entered password does not match the known password, wherein the user of the electronic device is blocked from network access other than the password reset tool while being redirected to the second server, wherein the second server is separate from the first server;

after redirecting the user of the electronic device to the second server providing the password reset tool, accepting user entry of verification information at the second server;

comparing the verification information from the user with known verification information for the user;

accepting user entry of a new password if the verification information accepted from the user matches the known verification information for the user; and

storing the new password as the known password for the user.

2. – 4. (canceled)

5. (currently amended) A method according to ~~Claim 4~~ Claim 1 wherein accepting ~~user~~ entry of the password from ~~a remote~~ the electronic device comprises accepting entry of the password from the ~~remote~~ electronic device over a telephone line.

6. (currently amended) A method according to ~~Claim 2~~ Claim 1 further comprising:

providing network service for the user without redirecting to the <u>second server providing</u> <u>the</u> password reset tool if the entered password matches the known password for the user.

7. (currently amended) A method according to ~~Claim 2~~ <u>Claim 1</u> wherein redirecting the user to ~~a~~ <u>the second server providing the</u> password reset tool comprises redirecting the user to the <u>second server providing the</u> password reset tool if a predetermined number of passwords have been accepted from the user during a session without matching the known password.

8. (currently amended) A method according to ~~Claim 2~~ <u>Claim 1</u> wherein accepting ~~user~~ entry of a password further comprises accepting ~~user~~ entry of a username and the password <u>from</u> <u>the electronic device</u>, and wherein redirecting the user <u>of the electronic device</u> to ~~a~~ <u>the</u> password reset tool if the password from the <u>electronic device</u> ~~user~~ does not match the known password further comprises redirecting the user <u>of the electronic device</u> to <u>the second server providing</u> the password reset tool only if the username <u>from the electronic device</u> ~~entered by the user~~ is a valid username.

9. (currently amended) A method according to Claim 1 further comprising:
terminating redirecting of the user <u>of the electronic device</u> to <u>the second server providing</u> the password reset tool if the verification information entered by the user does not match the known verification information.

10. (currently amended) A method according to Claim 1 further comprising:
terminating redirecting of the user <u>of the electronic device</u> to <u>the second server providing</u> the password reset tool if user verification information is accepted a predetermined number of times without matching the known verification information.

11. (currently amended) A method according to Claim 1 further comprising:
terminating redirecting of the user <u>of the electronic device</u> to <u>the second server providing</u> the password reset tool if a predetermined period of time passes without accepting user verification information matching the known verification information.

12. (currently amended) A method according to Claim 1 further comprising:

after accepting entry of the new password, terminating redirecting of the user of the electronic device to the second server providing the password reset tool.

13. (currently amended) A method according to Claim 1 further comprising:

after accepting entry of the new password from a the remote electronic device, transmitting instructions for the remote electronic device to automatically save the new password.

14. (currently amended) A method according to Claim 1 wherein redirecting the user of the electronic device to the second server providing the password reset tool comprises tunneling the user from the first server to the second server providing the password reset tool.

15. (currently amended) A method according to Claim 1 further comprising:

after redirecting the user of the electronic device to the second server providing the password reset tool, accepting a request for a network browser at the second server; and

responsive to accepting the request for an network browser, providing a password reset window including prompts for entry of the verification information while the user of the electronic device is blocked from network access other than the password reset tool wherein the password reset window is provided from the second server at the electronic device remote from the second server.

16. (currently amended) A method according to Claim 1 further comprising:

after redirecting the user of the electronic device to the second server providing the password reset tool, accepting a request for e-mail service at the second server from the electronic device; and

responsive to accepting the request for e-mail service, providing a password reset e-mail from the second server for the user including a link to a password reset window including

prompts for entry of the verification information <u>while the user of the electronic device is</u> <u>blocked from network access other than the password reset tool</u>.

17. (currently amended) A method according to Claim 16 further comprising:

responsive to accepting the request for e-mail, blocking access <u>of the user of the</u> <u>electronic device</u> to all e-mails other than the password reset e-mail.

18. (original) A method according to Claim 1 wherein the network service account comprises an Internet service account.

19. (currently amended) A network service system that provides access to a data network for a user having a network service account therewith, the system comprising:

<u>an access control point implemented on a first server configured to accept entry of a</u> <u>password from an electronic device remote from the first server as a condition of providing</u> <u>access to the data network, to compare the entered password with a known password for the user</u> <u>using the electronic device, and to redirect the user of the electronic device if the entered</u> <u>password does not match the known password; and</u>

a password reset tool <u>implemented on a second server separate from the first server,</u> <u>wherein the password reset tool is</u> configured to accept redirection of a <u>the</u> user <u>of the electronic</u> <u>device</u> thereto <u>from the access control point implemented at the first server to the password reset</u> <u>tool implemented at the second server</u>, wherein the user <u>of the electronic device</u> is blocked from network access other than the password reset tool <u>implemented at the second server</u> while being redirected, the password reset tool <u>implemented at the second server</u> being further configured to accept user entry of verification information after redirecting the user <u>of the electronic device</u> to the password <u>reset</u> tool, to compare the verification information from the user <u>of the electronic</u> <u>device</u> with known verification information for the user <u>of the electronic device</u>, to accept user entry of a new password if the verification information accepted from the user <u>of the electronic</u> <u>device</u> matches the known verification information for the user <u>of the electronic device</u>, and to store the new password as the known password for the user <u>of the electronic device</u>.

20. – 22. (canceled)

23. (currently amended) A network service system according to ~~Claim 22~~ Claim 19 wherein the access control point is configured to accept entry of the password from the ~~remote~~ electronic device over a telephone line.

24. (currently amended) A network service system according to ~~Claim 20~~ Claim 19 wherein the access control point is configured to provide network service for the user of the electronic device without redirecting to the password reset tool if the entered password matches the known password for the user.

25. (currently amended) A network service system according to ~~Claim 20~~ Claim 19 wherein the access control point is configured to redirect the user to the password reset tool if a predetermined number of passwords have been accepted from the user during a session without matching the known password.

26. (currently amended) A network service system according to ~~Claim 20~~ Claim 19 wherein the access control point is configured to accept user entry of a username and the password, and to redirect the user to the password reset tool only if the username entered by the user is a valid username.

27. (original) A network service system according to Claim 19 wherein the password reset tool is configured to terminate redirection of the user to the password reset tool if the verification information entered by the user does not match the known verification information.

28. (original) A network service system according to Claim 19 wherein the password reset tool is configured to terminate redirection of the user to the password reset tool if user verification information is accepted a predetermined number of times without matching the known verification information.

29. (original) A network service system according to Claim 19 wherein the password reset tool is configured to terminate redirection of the user to the password reset tool if a predetermined period of time passes without accepting user verification information matching the known verification information.

30. (original) A network service system according to Claim 19 wherein the password reset tool is configured to terminate redirection of the user to the password reset tool after accepting entry of the new password.

31. (currently amended) A network service system according to Claim 19 wherein the password reset tool is configured to transmit instructions for ~~a~~ the remote electronic device to automatically save the new password after accepting entry of the new password from the remote electronic ~~device,~~ device.

32. (currently amended) A network service system according to Claim 19 wherein the access control point implemented at the first server is configured to redirect the user of the electronic device by tunneling the user of the electronic device to the password reset tool, and wherein the password reset tool implemented at the second server is configured to accept tunneling of the user of the electronic device ~~to the password reset tool~~ from the access control point.

33. (currently amended) A network service system according to Claim 19 wherein the password reset tool implemented at the second server is configured to accept a request for a network browser after accepting redirection of the user of the electronic device, and to provide a password reset window including prompts for entry of the verification information responsive to accepting the request for an network browser while the user of the electronic device is blocked from network access other than the password reset tool wherein the password reset window is provided from the second server at the electronic device remote from the second server.

34. (currently amended) A network service system according to Claim 19 wherein the password reset tool is configured to accept a request for e-mail service after redirecting the user to the password reset tool implemented at the second server, and to provide a password reset e-mail for the user of the electronic device including a link to a password reset window including prompts for entry of the verification information responsive to accepting the request for e-mail service while the user of the electronic device is blocked from network access other than the password reset tool.

35. (currently amended) A network service system according to Claim 34 wherein the password reset tool is configured to block access of the user of the electronic device to all e-mails other than the password reset e-mail responsive to accepting the request for e-mail.

36. (original) A network service system according to Claim 19 wherein the network service account comprises an Internet service account.

37. (currently amended) A computer program product configured to reset a password for a network service account, the computer program product comprising a computer useable storage medium having computer-readable program code embodied in the medium, the computer-readable program code comprising:

computer-readable program code that is configured to accept entry of a password at a first server from an electronic device wherein the electronic device is remote from the first server; and

computer-readable program code that is configured to compare the entered password with a known password, wherein redirecting the user to the password reset tool comprises redirecting the user to the password reset tool if the entered password does not match the known password;

computer-readable program code that is configured to redirect the a user of the electronic device from the first server to a second server providing a password reset tool if the entered password does not match the known password after comparing the entered password with the known password, and to block the user of the electronic device from network access other than

the password reset tool while being redirected <u>to the second server, wherein the second server is separate from the first server</u>;

computer-readable program code that is configured to accept user entry of verification information <u>at the second server</u> after redirecting the user <u>of the electronic device</u> to the <u>second server providing the</u> password reset tool;

computer-readable program code that is configured to compare the verification information from the user with known verification information for the user;

computer-readable program code that is configured to accept user entry of a new password if the verification information accepted from the user matches the known verification information for the user; and

computer-readable program code that is configured to store the new password as the known password for the user.

38. – 40. (original)

41. (currently amended) A computer program product according to ~~Claim 40~~ <u>Claim 37</u> wherein accepting user entry of the password from ~~a remote~~ <u>the</u> electronic device comprises accepting entry of the password from the ~~remote~~ electronic device over a telephone line.

42. (currently amended) A computer program product according to ~~Claim 38~~ <u>Claim 37</u> further comprising:

computer-readable program code that is configured to provide network service for the user without redirecting to the <u>second server providing</u> password reset tool if the entered password matches the known password for the user.

43. (currently amended) A computer program product according to ~~Claim 38~~ <u>Claim 37</u> wherein redirecting the user to ~~a~~ <u>the second server providing the</u> password reset tool comprises redirecting the user to <u>the second server providing</u> the password reset tool if a predetermined number of passwords have been accepted from the user during a session without matching the known password.

44. (currently amended) A computer program product according to ~~Claim 38~~ Claim 37 wherein accepting ~~user~~ entry of a password further comprises accepting ~~user~~ entry of a username and the password <u>from the electronic device,</u> and wherein redirecting the user <u>of the electronic device</u> to ~~a~~ <u>the</u> password reset tool if the password from the <u>electronic device</u> ~~user~~ does not match the known password further comprises redirecting the user <u>of the electronic device</u> to <u>the second server providing</u> the password reset tool only if the username <u>from the electronic device</u> ~~entered by the user~~ is a valid username.

45. (currently amended) A computer program product according to Claim 37 further comprising:

computer-readable program code that is configured to terminate redirecting of the user <u>of the electronic device</u> to <u>the second server providing</u> the password reset tool if the verification information entered by the user does not match the known verification information.

46. (currently amended) A computer program product according to Claim 37 further comprising:

computer-readable program code that is configured to terminate redirecting of the user <u>of the electronic device</u> to <u>the second server providing</u> the password reset tool if user verification information is accepted a predetermined number of times without matching the known verification information.

47. (original) A computer program product according to Claim 37 further comprising:

computer-readable program code that is configured to terminate redirecting of the user <u>of the electronic device</u> to <u>the second server providing</u> the password reset tool if a predetermined period of time passes without accepting user verification information matching the known verification information.

48. (currently amended) A computer program product according to Claim 37 further comprising:

computer-readable program code that is configured to terminate redirecting of the user <u>of</u> <u>the electronic device</u> to <u>the second server providing</u> the password reset tool after accepting entry of the new password.

49. (currently amended) A computer program product according to Claim 37 further comprising:

computer-readable program code that is configured to transmit instructions for a <u>the</u> remote electronic device to automatically save the new password after accepting entry of the new password from the remote electronic device.

50. (currently amended) A computer program product according to Claim 37 wherein redirecting the user <u>of the electronic device</u> to <u>the second server providing</u> the password reset tool comprises tunneling the user <u>from the first server</u> to <u>the second server providing</u> the password reset tool.

51. (currently amended) A computer program product according to Claim 37 further comprising:

computer-readable program code that is configured to accept a request for a network browser <u>at the second server</u> after redirecting the user <u>of the electronic device</u> to <u>the second</u> <u>server providing</u> the password reset tool; and

computer-readable program code that is configured to ~~providing~~ <u>provide</u> a password reset window including prompts for entry of the verification information responsive to accepting the request for a network browser <u>while the user of the electronic device is blocked from</u> <u>network access other than the password reset tool wherein the password reset window is</u> <u>provided from the second server at the electronic device remote from the second server</u>.

52. (currently amended) A computer program product according to Claim 37 further comprising:

computer-readable program code that is configured to accept a request for e-mail service at the second server from the electronic device after redirecting the user of the electronic device to the second server providing the password reset tool; and

computer-readable program code that is configured to provide a password reset e-mail from the second server for the user including a link to a password reset window including prompts for entry of the verification information responsive to accepting the request for e-mail service while the user of the electronic device is blocked from network access other than the password reset tool.

53. (currently amended) A computer program product according to Claim 52 further comprising:

computer-readable program code that is configured to block access of the user of the electronic device to all e-mails other than the password reset e-mail responsive to accepting the request for e-mail.

54. (original) A computer program product according to Claim 37 wherein the network service account comprises an Internet service account.

55. – 56. (canceled)

57. (new) A method according to Claim 1 wherein the electronic device is remote from both of the first and second servers.

58. (new) A method according to Claim 1 wherein the second server comprises an element of a sandbox network and wherein the first server is outside the sandbox network.

59. (new) A network service system according to Claim 19 wherein the electronic device is remote from both of the first and second servers.

60. (new) A network service system method according to Claim 19 wherein the second server comprises an element of a sandbox network and wherein the first server is outside the sandbox network.

61. (new) A computer program product according to Claim 37 wherein the electronic device is remote from both of the first and second servers.

62. (new) A computer program product according to Claim 37 wherein the second server comprises an element of a sandbox network and wherein the first server is outside the sandbox network.